Monthly Cybersecurity Newsletter

July 2024

NCDIT | NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Enterprise Security and Risk Management Office (ESRMO)

From the Desk of the State Chief Risk Officer – Torry Crass

Upcoming Events to Focus on Business Continuity Planning

Beginning July 1, the N.C. Department of Information Technology's Enterprise Security and Risk Management Office will host several events dedicated to business continuity planning.

These events are designed to strengthen resilience across the state and promote the development and review of business plans. The schedule of events are as follows:

- **July 1:** Formal kickoff for start of agencies annual Business Continuity Plan reviews
- **July 10-11:** Business Continuity Training (virtual, in-person optional)
- **Oct. 31:** Due date to submit agency Business Continuity Plans

For more information, send an email to bcm@nc.gov.

New Money-Stealing Malware Targets Google Chrome and Microsoft Word

Cybersecurity experts have issued a stark warning about a new malware strain designed to steal money by targeting users of Google Chrome and Microsoft Word. This sophisticated malware exploits vulnerabilities in these widely used applications to gain unauthorized access to sensitive financial information.

According to recent reports from BleepingComputer and TechRadar, the malware operates by embedding malicious code within seemingly legitimate documents and web extensions. When users open an infected Microsoft Word document or install a compromised Google Chrome extension, the malware silently installs itself on their devices. From there, it can monitor and capture keystrokes, access saved passwords and even intercept financial transactions.

Let's take a deeper look into how this works.

The malware typically arrives through phishing emails containing infected Word documents or through malicious Chrome extensions posing as useful tools. This is the delivery mechanism of the cyber kill chain.

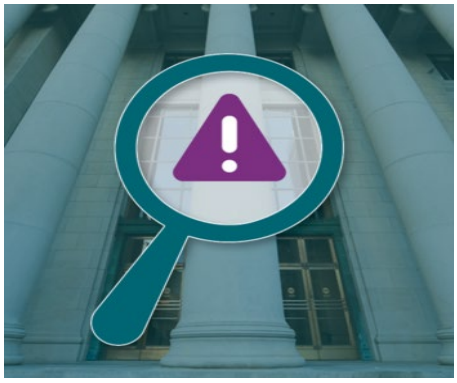
Once opened or installed, the malware embeds itself within the system, bypassing traditional security measures. It then captures keystrokes, screenshots and browser activity, focusing on financial websites and applications. The collected data is transmitted to the attackers, who use it to steal money directly from victims' accounts or sell the information on the dark web.

Cybersecurity experts consistently advise users to take several precautions to safeguard against this growing threat.

- Be cautious of unsolicited emails and avoid opening email attachments or clicking on links from unknown sources.
- Only install browser extensions from trusted developers and ensure their authenticity before installation.
- Keep all software, including Google Chrome and Microsoft Word, updated with the latest security patches.
- Use robust antivirus and anti-malware solutions to detect and block potential threats.
- Enable multifactor authentication for additional security on financial accounts.

By following expert advice and maintaining good security practices, users can significantly reduce the risk of falling victim.

Phishing Campaign Abuses Windows Search to Distribute Malware



Researchers at Trustwave warn that a phishing campaign is distributing malware via HTML attachments disguised as invoices. Notably, the HTML files abuse the Windows search protocol to launch Windows Explorer and trick users into installing the malware.

“We found the threat actors utilizing a sophisticated understanding of system vulnerabilities and user behaviors” the researchers state. “The campaign starts with a suspicious email containing an HTML attachment disguised as a routine document, like an invoice. The threat actor encloses the HTML file within a ZIP archive to enhance deception and evade email security scanners.”

When the user opens the HTML file, they’ll be prompted to allow the search function. The function will attempt to trick the user into running a malicious script.

“The attack moves to its next phase after the user permits the search action,” Trustwave explains. “The search function retrieves invoice-named files from a remote server. Only one item, particularly a shortcut (LNK) file, appears in the search results. This LNK file points to a batch script (BAT) hosted on the same server, which, upon user click, could potentially trigger additional malicious operations.”

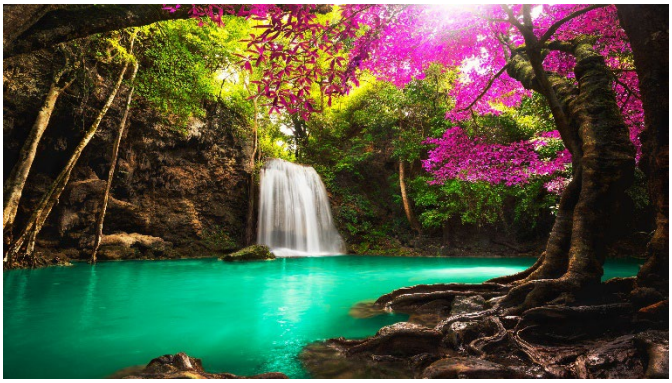
Trustwave concludes that user awareness is necessary to thwart evolving social engineering tactics.

“The HTML document serves as a crucial component in this attack, facilitating the execution of a script that exploits the Windows search functionality,” the researchers write. “While this attack does not utilize automated installation of malware, it does require users to engage with various prompts and clicks.

However, this technique cleverly obscures the attacker’s true intent, exploiting the trust users place in familiar interfaces and common actions like opening email attachments. As users continue to navigate an increasingly complex threat landscape, ongoing education, and proactive security strategies remain paramount in safeguarding against such deceptive tactics.”

This article is redistributed with permission from KnowBe4.

Vacation-Themed Scams Are Spiking



Scammers are now impersonating legitimate services like Booking.com and Kayak to target people planning their summer vacations. One out of every 33 vacation-themed domains registered last month was malicious, researchers at Check Point warn.

“In May 2024, Check Point Research detected a significant surge in summer-related cyber scams, highlighting the need for travelers to stay informed and proactive in safeguarding their personal information,” the researchers write.

“Specifically, a notable surge in newly created domains related to holidays or vacations was observed, with a significant increase compared to the same period last year. Out of the 25,668 new domains registered, one out of every 33 was found to be either malicious or suspicious.”

Check Point offers the following advice to help users avoid falling for these scams:

- Verify website authenticity by checking for HTTPS in the URL, and look for trust indicators such as padlock symbols or site seals. Avoid entering personal information on websites with suspicious URLs or those with misspellings
- Exercise caution with emails, even those seemingly from reputable sources. Be wary of unexpected attachments or requests for personal information. When in doubt, contact the company directly using contact information from their official website instead of clicking on links in the email
- Stay informed about the latest cybersecurity threats and scams by following reputable cybersecurity blogs, subscribing to security newsletters and participating in online forums or communities where cybersecurity professionals share insights and advice
- Use comprehensive security software such as antivirus and anti-malware programs to regularly scan your devices for threats. Keep these programs updated with the latest definitions to ensure they can detect and prevent new forms of malware”

This article is redistributed with permission from KnowBe4.

Software Managing Auto Sales and Services Hit by Cyberattack

In recent editions of the Monthly Cybersecurity Newsletter, we discussed cyberattacks on the healthcare systems in the United States. It now appears that other industries are also being targeted.

The auto industry was the most recent target in the latest attacks. There is no proof as to whether these incidents are linked.

The incident was first discovered around the first half of June, when a major software platform managing auto sales and services was compromised. This caused significant disruption across the automotive industry affecting thousands of car dealerships, repair shops and related service providers that rely on the software for daily operations.

The attack targeted a widely used software system designed to streamline various aspects of auto sales and service management, including customer relationship management (CRM), inventory tracking, appointment scheduling and financial transactions. Hackers gained unauthorized access to sensitive data after exploiting a vulnerability in the software allowing them to cripple the system's functionality.

The breach has had immediate and far-reaching consequences. Dealerships have reported difficulties in processing sales, tracking inventory and managing customer interactions. Repair shops have faced challenges in scheduling appointments and accessing service histories, leading to delays and frustrated customers. Financial transactions, including loan processing and payment handling, have also been disrupted, causing significant financial strain on businesses.

In response to the attack, the software provider has taken steps to contain the breach and restore functionality. They have partnered with cybersecurity experts to investigate the incident, patch the exploited vulnerability and implement enhanced security measures to prevent future attacks. Affected businesses are being advised on how to safeguard their systems and protect customer data in the interim.

Customers of affected auto dealerships and service centers are being urged to monitor their accounts for any suspicious activity. The compromised data may include personal information, financial details and vehicle history records. Businesses are required to notify customers of the breach and provide guidance on how to protect themselves from potential fraud.

As the automotive sector continues to embrace technological advancements, the importance of enhancing cybersecurity measures cannot be overstated. Businesses must prioritize the protection of their digital infrastructure to safeguard against future attacks and ensure the continuity of their operations.

City of Clevland Hit by Ransomware Attack

On June 18, the city of Cleveland became the latest victim of a sophisticated ransomware attack, disrupting several municipal services and raising concerns about cybersecurity in public institutions.

The attack, which targeted the city's IT infrastructure, led to the encryption of critical data, rendering several online services and internal systems inoperable.

Residents reportedly had issues accessing public records, paying utility bills online and scheduling services. The city's emergency services, however, remained operational, with contingency measures ensuring that police, fire and medical responses were unaffected.

City officials quickly issued statements to reassure residents, emphasizing that they were working with cybersecurity experts and federal agencies to address the situation. The city’s mayor urged residents to be patient and cautious, particularly with unsolicited emails or phone calls, which could be phishing attempts related to the attack.

In response to the attack, the city's IT department isolated the affected systems to prevent the spread of the malware. A comprehensive investigation was launched in collaboration with the FBI and cybersecurity firms to identify the origin of the attack and the specific ransomware variant used.

Experts from the Cybersecurity and Infrastructure Security Agency were called in to assist in the recovery process. The primary goal was to restore essential services and recover encrypted data without paying the ransom, as paying often does not guarantee the return of data and can encourage further criminal activity.

Cities and municipalities, often with constrained budgets for cybersecurity, have become prime targets for cybercriminals seeking quick financial gains.

As Cleveland works to recover from this attack, other cities are taking note and ramping up their cybersecurity efforts. The incident highlights the need for increased funding and resources dedicated to protecting critical infrastructure from cyber threats.

The city of Cleveland's experience will likely contribute to a broader national conversation about the importance of cybersecurity in the public sector, emphasizing that preparedness and resilience are key to mitigating the impact of such attacks in the future.

Training & Continued Learning Resources

- FedVTE: Free Online Training Environment: https://fedvte.usalearning.gov/
- TEEX: Texas Engineering Extension Service: https://teex.org/
- NICCS: National Initiative for Cybersecurity Careers & Studies: https://niccs.cisa.gov/
- ICS-CERT Training: https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT

CYBERSECURITY NEWSLETTERS

SAC Security Awareness Newsletter: Monthly security awareness newsletter provided for all state employees by KnowBe4. Access the newsletter. ***Note:*** *You must have a valid state employee Microsoft 365 account.*

CIS Security Tips Newsletter: Free monthly cybersecurity resource from the Center for Internet Security. https://www.cisecurity.org/insights/newsletter

SANS OUCH! Newsletter: Free monthly cybersecurity awareness newsletter provided by the SANS Institute. https://www.sans.org/newsletters/ouch/

Upcoming Training & Events

- **Jul 5:** SANS Webinar: Do You Think You're Ready to Attack the Cloud? Unlock the Secrets of Cloud Penetration Testing!
- **Jul 9:** SANS Webinar: Practical Threat Modeling Based on Community Templates
- **Jul 10:** SANS Webinar: Everything is a file. Or is it?
- **Jul 10:** SANS Webinar: Advanced Forensics Workshop: Handling AI and Unsupported Apps in Smartphone Investigations
- **Jul 12:** SANS Webinar: Data Carving: Recovering Hidden Files from Digital Graveyards
- **Jul 17:** SANS Webinar: Process Code Injection - Detection, Response, and Mitigation

View a list of upcoming SANS webcasts.

Be sure to follow the N.C. Department of Information Technology on X (formerly known as Twitter), Facebook and LinkedIn for more tips. Also visit it.nc.gov/CyberSecureNC or Stay Safe Online for additional information and resources on cybersecurity awareness. Remember … Stop. Think. Connect.

Disclaimer: Vendors, references and links in this newsletter are for informational purposes only, and their inclusion should, in no way, be considered an endorsement from the N.C. Department of Information Technology.